

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-109856

(43)公開日 平成11年(1999) 4月23日

(51)Int.Cl.<sup>9</sup>  
G 0 9 C 1/00  
G 0 6 F 9/06  
12/14  
H 0 4 L 9/08

識別記号  
6 3 0  
5 5 0  
3 2 0

F I  
G 0 9 C 1/00  
G 0 6 F 9/06  
12/14  
H 0 4 L 9/00  
6 3 0 A  
5 5 0 A  
3 2 0 B  
6 0 1 A

審査請求 未請求 請求項の数14 O L (全 10 頁)

(21)出願番号 特願平9-267515  
(22)出願日 平成9年(1997) 9月30日

(71)出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(71)出願人 390020248  
日本テキサス・インスツルメンツ株式会社  
東京都港区北青山3丁目6番12号 青山富士ビル  
(72)発明者 金光 朋彦  
大阪府門真市大字門真1006番地 松下電器産業株式会社内  
(74)代理人 弁理士 山本 秀策

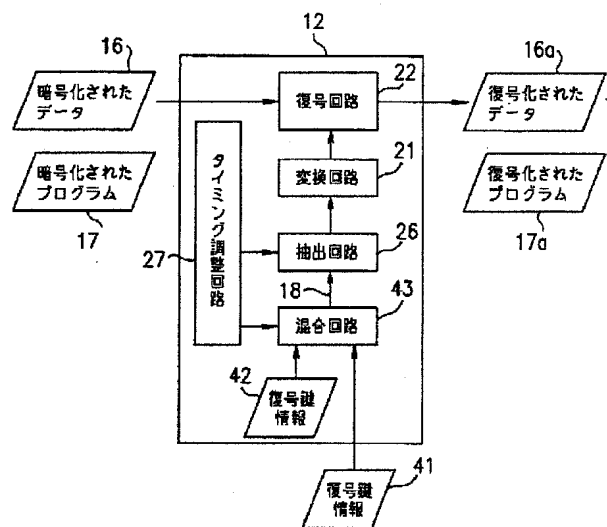
最終頁に続く

(54)【発明の名称】 復号装置

(57)【要約】

【課題】 復号鍵情報を不正に取得した第三者が暗号化されたプログラムまたは暗号化されたデータを容易に復号化することを防止する。

【解決手段】 復号装置12は、復号鍵情報41と復号鍵情報42とに基づいて、復号鍵18aを生成する復号鍵生成回路(43、26、21)と、復号鍵18aを用いて暗号化された情報を復号化する復号回路22とを備えている。復号鍵情報41は、復号装置12の外部から入力される。復号鍵情報42は、復号装置12の内部に格納されている。



## 【特許請求の範囲】

【請求項1】 第1復号鍵情報と第2復号鍵情報とに基づいて、復号鍵を生成する復号鍵生成回路と、前記復号鍵を用いて、暗号化された情報を復号化する復号回路とを備えた復号装置であって、前記第1復号鍵情報は、前記復号装置の外部から入力され、前記第2復号鍵情報は、前記復号装置の内部に格納されている、復号装置。

【請求項2】 前記暗号化された情報は、暗号化されたプログラムである、請求項1に記載の復号装置。

【請求項3】 前記暗号化された情報は、暗号化されたデータである、請求項1に記載の復号装置。

【請求項4】 前記復号鍵生成回路は、前記第1復号鍵情報と前記第2復号鍵情報とを混合することにより、復号鍵情報を生成する混合回路と、前記復号鍵情報を前記復号鍵に変換する変換回路とを含む、請求項1に記載の復号装置。

【請求項5】 前記第1復号鍵情報は、前記復号鍵に関連する情報と前記復号鍵に関連しないダミーデータとを含む、請求項1に記載の復号装置。

【請求項6】 前記第2復号鍵情報は、複数の復号鍵を含んでおり、前記復号鍵生成回路は、前記複数の復号鍵のうち1つを選択する選択回路を含む、請求項1に記載の復号装置。

【請求項7】 前記第2復号鍵情報は、複数の復号鍵情報を含んでおり、前記復号鍵生成回路は、前記複数の復号鍵情報のうち1つを選択する選択回路と、前記選択回路によって選択された復号鍵情報を復号鍵に変換する変換回路とを含む、請求項1に記載の復号装置。

【請求項8】 復号鍵情報を復号鍵に変換する第1変換回路と、前記復号鍵を用いて、暗号化された情報を復号化する復号回路とを備え、前記復号鍵情報は、前記復号鍵に関連する情報と前記復号鍵に関連しないダミーデータとを含む、復号装置。

【請求項9】 前記暗号化された情報は、暗号化されたプログラムである、請求項8に記載の復号装置。

【請求項10】 前記暗号化された情報は、暗号化されたデータである、請求項8に記載の復号装置。

【請求項11】 前記復号鍵に関連する情報は、前記復号鍵を含んでおり、前記第1変換回路は、前記復号鍵情報から前記復号鍵を抽出する抽出回路を含む、請求項8に記載の復号装置。

【請求項12】 前記第1変換回路は、前記復号鍵情報から前記復号鍵に関連する情報を抽出する抽出回路と、

前記復号鍵に関連する情報を前記復号鍵に変換する第2変換回路とを含む、請求項8に記載の復号装置。

【請求項13】 前記暗号化された情報は、前記復号装置に関連して設けられたメモリに格納されている、請求項1または請求項8のいずれかに記載の復号装置。

【請求項14】 前記復号装置は、入力されたアドレスを一定の規則に従って変換し、変換されたアドレスを前記メモリに出力するアドレスシャッフル回路をさらに備えており、前記変換されたアドレスに従って前記メモリから読み出された前記暗号化された情報が前記復号回路に供給される、請求項13に記載の復号装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、復号鍵を用いて暗号化されたプログラムまたは暗号化されたデータを復号化する復号装置に関する。

## 【0002】

【従来の技術】従来、データを暗号化して保存し、そのデータを暗号化するのに使用した鍵をマスタ鍵を用いて暗号化して保存する手法が提案されている（例えば、辻井重男、笠原正雄著「暗号と情報セキュリティ」、第208頁～第212頁、昭晃堂、1990年）。

【0003】上記文献は、そのように暗号化されたデータを復号化する復号装置を開示している。復号装置には、暗号化されたデータとマスタ鍵 $K_M$ とが入力される。復号装置は、暗号化されたデータのヘッダ部分にある鍵 $K_E$ を抽出し、鍵 $K_E$ をレジスタに格納する。復号装置は、鍵 $K_E$ とマスタ鍵 $K_M$ とに基づいてワーク鍵 $K_W$ を生成し、ワーク鍵 $K_W$ を用いて暗号化されたデータを復号化する。

【0004】このような復号装置をプロセッサの内部に持つこととすると、外部から参照できるのは、暗号化されたデータと、暗号化された鍵 $K_M$ と、マスタ鍵 $K_M$ とである。従って、マスタ鍵 $K_M$ を機密に管理することにより、暗号化されたデータを保護することができる。

## 【0005】

【発明が解決しようとする課題】しかしながら、上述した従来技術によれば、マスタ鍵 $K_M$ とワーク鍵 $K_W$ の間に相関があるので、マスタ鍵 $K_M$ がわかってしまうと、暗号化アルゴリズムが既知の場合には暗号化されたデータが比較的容易に復号化してしまうという問題点があった。

【0006】このため、従来では、マスタ鍵 $K_M$ の機密レベルを高く設定する必要があった。このことは、マスタ鍵 $K_M$ を復号装置に転送するために必要とされる回路の規模を増大させるという問題点があった。

【0007】本発明は、上記問題点を鑑みてなされたものであり、復号鍵情報を不正に取得した第三者が暗号化されたプログラムまたは暗号化されたデータを容易に復号化することを防止する復号装置を提供することを目的

とする。また、復号鍵情報を復号装置に転送するために必要とされる回路の規模を削減することのできる復号装置を提供することを目的とする。

【0008】

【課題を解決するための手段】本発明の復号装置は、第1復号鍵情報と第2復号鍵情報とに基づいて、復号鍵を生成する復号鍵生成回路と、前記復号鍵を用いて、暗号化された情報を復号化する復号回路とを備え、前記第1復号鍵情報は、前記復号装置の外部から入力され、前記第2復号鍵情報は、前記復号装置の内部に格納されている。これにより、上記目的が達成される。

【0009】前記暗号化された情報は、暗号化されたプログラムであってもよい。

【0010】前記暗号化された情報は、暗号化されたデータであってもよい。

【0011】前記復号鍵生成回路は、前記第1復号鍵情報と前記第2復号鍵情報とを混合することにより、復号鍵情報を生成する混合回路と、前記復号鍵情報を前記復号鍵に変換する変換回路とを含んでいてもよい。

【0012】前記第1復号鍵情報は、前記復号鍵に関連する情報と前記復号鍵に関連しないダミーデータとを含んでいてもよい。

【0013】前記第2復号鍵情報は、複数の復号鍵を含んでおり、前記復号鍵生成回路は、前記複数の復号鍵のうち1つを選択する選択回路を含んでいてもよい。

【0014】前記第2復号鍵情報は、複数の復号鍵情報を含んでおり、前記復号鍵生成回路は、前記複数の復号鍵情報のうち1つを選択する選択回路と、前記選択回路によって選択された復号鍵情報を復号鍵に変換する変換回路とを含んでいてもよい。

【0015】本発明の他の復号装置は、復号鍵情報を復号鍵に変換する第1変換回路と、前記復号鍵を用いて、暗号化された情報を復号化する復号回路とを備え、前記復号鍵情報は、前記復号鍵に関連する情報と前記復号鍵に関連しないダミーデータとを含む。これにより、上記目的が達成される。

【0016】前記暗号化された情報は、暗号化されたプログラムであってもよい。

【0017】前記暗号化された情報は、暗号化されたデータであってもよい。

【0018】前記復号鍵に関連する情報は、前記復号鍵を含んでおり、前記第1変換回路は、前記復号鍵情報から前記復号鍵を抽出する抽出回路を含んでいてもよい。

【0019】前記第1変換回路は、前記復号鍵情報から前記復号鍵に関連する情報を抽出する抽出回路と、前記復号鍵に関連する情報を前記復号鍵に変換する第2変換回路とを含んでいてもよい。

【0020】前記暗号化された情報は、前記復号装置に関連して設けられたメモリに格納されていてもよい。

【0021】前記復号装置は、入力されたアドレスを

定の規則に従って変換し、変換されたアドレスを前記メモリに出力するアドレスシャッフル回路をさらに備えており、前記変換されたアドレスに従って前記メモリから読み出された前記暗号化された情報が前記復号回路に供給されてもよい。

【0022】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を説明する。

【0023】（実施の形態1）図1は、本発明の復号装置12を含むプロセッサチップ11の構成を示す。プロセッサチップ11は、復号装置12とインタフェース13とプロセッサコア15とを含む。

【0024】復号鍵情報18は、インタフェース13およびバス14を介して、復号装置12に入力される。インタフェース13は、復号鍵情報の入力に特化されたものである必要はない。例えば、インタフェース13は、プロセッサチップ11内に設けられている各種のレジスタ（図示せず）に設定する値19などを入力するためにも使用され得る。

【0025】暗号化されたデータ16は、復号装置12に入力される。復号装置12は、復号鍵情報18を用いて、暗号化されたデータ16を復号化する。復号化されたデータはプロセッサコア15に供給される。復号鍵情報18および復号処理の詳細は、図2（a）～（c）を参照して後述される。

【0026】暗号化されたプログラム17は、復号装置12に入力される。復号装置12は、復号鍵情報18を用いて、暗号化されたプログラム17を復号化する。復号化されたプログラムはプロセッサコア15に直接的に供給される。あるいは、復号化されたプログラムはプログラムローダ（図示せず）に供給されてもよい。復号化されたプログラムが実行されると、プロセッサチップ11内に設けられているプログラムメモリ（図示せず）や各種のレジスタ（図示せず）に値が設定される。

【0027】なお、暗号化されたデータ16と暗号化されたプログラム17とがプロセッサチップ11に同時に入力される形態も考えられる。この場合、例えば、復号装置12を2個並列に配置し、暗号化されたデータ16を一方の復号装置に入力し、暗号化されたプログラム17を他方の復号装置に入力するようにすればよい。

【0028】図2（a）は、復号装置12の構成を示す。復号装置12は、復号鍵情報18から復号鍵に関連する情報を抽出する抽出回路26と、抽出回路26によって抽出された復号鍵に関連する情報を復号鍵に変換する変換回路21と、復号鍵を用いて暗号化されたデータ16または暗号化されたプログラム17を復号化する復号回路22とを含んでいる。

【0029】復号鍵情報18は、復号鍵に関連する情報と、復号鍵に関連しないダミーデータとを含んでいる。復号鍵に関連する情報は、復号鍵自身であってもよい

し、復号鍵と相関を持った値であってもよい。

【0030】図2(b)は、復号鍵情報18の構成例を示す。復号鍵情報18は、復号鍵18aと、復号鍵18aに関連しないダミーデータ18bとを含む。復号鍵情報18における復号鍵18aの位置は予め決められている。復号鍵18aの位置は、例えば、復号鍵情報18の先頭から50バイト目であり得る。復号鍵情報18において、復号鍵18a以外の部分をダミーデータ18bで埋めることにより、仮に第三者が復号鍵情報18を得た場合でも復号鍵情報18の中から復号鍵18aを特定することは困難である。

【0031】図2(c)は、復号鍵情報18の他の構成例を示す。復号鍵情報18は、復号鍵18aと相関を持った値18c(以下、相関値18cという)と、復号鍵18aに関連しないダミーデータ18bとを含む。復号鍵情報18における相関値18cの位置は予め決められている。相関値18cの位置は、例えば、復号鍵情報18の先頭から50バイト目であり得る。復号鍵情報18において、相関値18c以外の部分をダミーデータ18bで埋めることにより、仮に第三者が復号鍵情報18を得た場合でも復号鍵情報18の中から相関値18cを特定することは困難である。

【0032】このように、復号鍵18aに関連しないダミーデータを使用することにより、復号鍵情報18の秘匿性を高めることができる。これにより、復号鍵情報18の機密レベルを下げるができる。その結果、復号鍵情報18を復号装置12に転送するために必要とされる回路の規模を削減することができる。

【0033】図2(a)を再び参照して、復号鍵情報18が入力された場合の復号装置12の動作を説明する。

【0034】図2(b)に示す構成を有する復号鍵情報18が入力された場合には、抽出回路26は、復号鍵情報18から復号鍵18aを抽出する。復号鍵18aを抽出するタイミングは、タイミング調整回路27から出力されるイネーブル信号によって制御される。抽出回路26によって抽出された復号鍵18aは、変換回路21をスルーして復号回路22に供給される。従って、復号鍵情報18が図2(b)に示す構成を有する場合には、変換回路21は省略され得る。復号回路22は、復号鍵18aを用いて暗号化されたデータ16または暗号化されたプログラム17を復号化する。その結果、復号化されたデータ16aまたは復号化されたプログラム17aが復号回路22から出力される。

【0035】図2(c)に示す構成を有する復号鍵情報18が入力された場合には、抽出回路26は、復号鍵情報18から相関値18cを抽出する。相関値18cを抽出するタイミングは、タイミング調整回路27から出力されるイネーブル信号によって制御される。抽出回路26によって抽出された相関値18cは、変換回路21に供給される。変換回路21は、相関値18cを復号鍵1

8aに変換する。ここで、復号鍵18aを正しく得るためには、相関値18cが所定の規則に従って復号鍵18aを導くことができる値であり、かつ、その所定の規則が変換回路21に予め反映されていることが必要とされる。例えば、相関値18cが復号鍵18aを可逆変換した値である場合には、相関値18cから復号鍵18aを導く式が変換回路21に設定されている必要がある。復号回路22は、復号鍵18aを用いて暗号化されたデータ16または暗号化されたプログラム17を復号化する。その結果、復号化されたデータ16aまたは復号化されたプログラム17aが復号回路22から出力される。

【0036】図3は、抽出回路26に入力される復号鍵情報18のタイミングとタイミング調整回路27から出力されるイネーブル信号のタイミングとの関係を示す。図3に示すように、イネーブル信号がHighである期間中、復号鍵情報18から復号鍵18a(または相関値18c)が切り出され、その切り出されたデータが変換回路21に供給される。

【0037】(実施の形態2)図4は、復号装置12の他の構成を示す。復号装置12とその周辺回路との関係は、図1に示すとおりである。

【0038】図4に示される復号装置12は、復号鍵情報41と復号鍵情報42とを混合することにより、復号鍵情報18を生成する混合回路43と、復号鍵情報18から復号鍵に関連する情報を抽出する抽出回路26と、抽出回路26によって抽出された復号鍵に関連する情報を復号鍵に変換する変換回路21と、復号鍵を用いて暗号化されたデータ16または暗号化されたプログラム17を復号化する復号回路22とを含んでいる。

【0039】復号鍵情報41は、復号装置12の外部から入力される。一方、復号鍵情報42は、復号装置12の内部に格納されている。復号鍵情報42を復号装置12の内部に格納するために、例えば、復号鍵情報42をプロセッサチップ11に設けられているROM(図示せず)に格納するようにしてもよい。あるいは、復号鍵情報42をハードワイヤードロジックを用いて復号装置12の内部に記憶するようにしてもよい。

【0040】このように、復号鍵を生成するために使用される情報の一部(すなわち、復号鍵情報42)が復号装置12の内部に格納されているため、第三者が復号鍵情報42を不正に取得することは困難である。第三者が復号鍵情報42を不正に取得するためには、第三者は電子顕微鏡などを用いて復号装置12の内部の回路を読みとらなければならないからである。近年、LSIのプロセスルールは微細化し、回路規模も増大する傾向にある。従って、復号装置12の内部の回路を読みとる作業はきわめて困難である。復号鍵情報42をROMに格納する方法と、復号鍵情報42をハードワイヤードロジックを用いて復号装置12の内部に記憶する方法とを比較

すると、前者は後者に比べて回路規模が小さくすむという利点を有するが、第三者が電子顕微鏡などを用いて回路を読みとることが容易であるという欠点を有する。従って、復号鍵情報42の秘匿性を高めるためには後者の方法を採用することが好ましい。

【0041】また、復号鍵を生成するために使用される情報の一部（すなわち、復号鍵情報42）が復号装置12の内部に格納されているため、第三者が復号鍵情報41を得た場合でも復号鍵を知ることは困難である。復号鍵は、復号鍵情報41と復号鍵情報42とに基づいて生成されるからである。これにより、復号装置12の外部から入力される復号鍵情報41の機密レベルを下げる事ができる。その結果、復号鍵情報41を復号装置12に転送するために必要とされる回路の規模を削減することができる。

【0042】次に、図4を参照して、復号鍵情報41が入力された場合の復号装置12の動作を説明する。

【0043】混合回路43は、復号鍵情報41と復号鍵情報42とを混合することにより、復号鍵情報18を生成する。復号鍵情報18は、例えば、図2(b)に示す構成を有する。あるいは、復号鍵情報18は、図2

(c)に示す構成を有していてもよい。抽出回路26、変換回路21、復号回路22およびタイミング制御回路27の動作は、図2(a)を参照して説明したそれらの動作と同一である。

【0044】復号鍵情報18を正しく得るためには、復号鍵情報18が所定の規則に従って復号鍵情報41と復号鍵情報42とに分割されており、かつ、その所定の規則が混合回路43に予め反映されていることが必要とされる。例えば、復号鍵情報18が100バイトのデータである場合、復号鍵情報18の前半50バイトのデータを復号鍵情報41として復号装置12の外部から入力し、復号鍵情報18の後半50バイトのデータを復号鍵情報42として復号装置12の内部に格納するにしてもよい。この場合には、混合回路43は、復号鍵情報41(50バイト)の末尾に復号鍵情報42(50バイト)を結合することにより、復号鍵情報18(100バイト)を生成する。なお、復号鍵情報18を復号鍵情報41と復号鍵情報42とに分割する方法としては、任意の方法を採用することができる。

【0045】図5は、復号装置12の他の構成を示す。復号装置12とその周辺回路との関係は、図1に示すとおりである。

【0046】図5に示される復号装置12は、復号鍵選択情報55に応じて復号鍵 $\alpha$ 、復号鍵 $\beta$ 、復号鍵 $\gamma$ のうちの1つを選択する選択回路54と、選択回路54によって選択された復号鍵を用いて暗号化されたデータ16または暗号化されたプログラム17を復号化する復号回路22とを含んでいる。

【0047】復号鍵選択情報55は、復号装置12の外

部から入力される。一方、復号鍵 $\alpha$ 、復号鍵 $\beta$ 、復号鍵 $\gamma$ は、いずれも、復号装置12の内部に格納されている。復号鍵 $\alpha$ 、復号鍵 $\beta$ 、復号鍵 $\gamma$ を復号装置12の内部に格納する方法としては、上述した復号鍵情報42を復号装置12の内部に格納する方法と同様の方法が採用され得る。例えば、復号鍵 $\alpha$ 、復号鍵 $\beta$ 、復号鍵 $\gamma$ をプロセッサチップ11に設けられているROM(図示せず)に格納する場合には、復号鍵 $\alpha$ はROMの格納位置51に格納され、復号鍵 $\beta$ はROMの格納位置52に格納され、復号鍵 $\gamma$ はROMの格納位置53に格納され得る。

【0048】このように、復号鍵を生成するために使用される情報の一部（すなわち、復号鍵 $\alpha$ 、復号鍵 $\beta$ 、復号鍵 $\gamma$ ）が復号装置12の内部に格納されているため、第三者が復号鍵選択情報55を得た場合でも復号鍵を知ることは困難である。復号鍵選択情報55の値は、復号鍵 $\alpha$ 、復号鍵 $\beta$ 、復号鍵 $\gamma$ の値とは無関係な値とすることができるからである。これにより、復号装置12の外部から入力される復号鍵選択情報55の機密レベルを下げる事ができる。その結果、復号鍵選択情報55を復号装置12に転送するために必要とされる回路の規模を削減することができる。

【0049】次に、図5を参照して、復号鍵選択情報55が入力された場合の復号装置12の動作を説明する。

【0050】選択回路54は、復号鍵選択情報55に応じて、復号鍵 $\alpha$ 、復号鍵 $\beta$ 、復号鍵 $\gamma$ のうちの1つを選択する。例えば、選択回路54は、復号鍵選択情報55が値0を有する場合に復号鍵 $\alpha$ を選択し、復号鍵選択情報55が値1を有する場合に復号鍵 $\beta$ を選択し、復号鍵選択情報55が値2を有する場合に復号鍵 $\gamma$ を選択する。復号鍵選択情報55の値と選択されるべき復号鍵との対応関係は任意に設定され得る。復号回路22は、選択回路54によって選択された復号鍵を用いて暗号化されたデータ16または暗号化されたプログラム17を復号化する。その結果、復号化されたデータ16aまたは復号化されたプログラム17aが復号回路22から出力される。

【0051】なお、復号装置12の内部に格納される復号鍵の数は3に限定されない。復号装置12の内部に格納される復号鍵の数は任意の正の整数であり得る。

【0052】なお、復号鍵の代わりに、復号鍵とダミーデータとを含む復号鍵情報を復号装置12の内部に格納するようにしてもよい。この場合には、復号鍵情報から復号鍵を抽出する抽出回路を復号回路22の前段に設ければよい。また、復号鍵選択情報55がダミーデータを含んでいてもよい。この場合には、復号鍵選択情報55から復号鍵に対応する値を抽出する抽出回路を選択回路54の前段に設ければよい。

【0053】図6は、復号装置12の他の構成を示す。復号装置12とその周辺回路との関係は、図1に示すと

おりである。

【0054】図6に示される復号装置12は、復号鍵選択情報55に応じて復号鍵と相関を持つ値 $\alpha$ （以下、相関値 $\alpha$ という）、復号鍵と相関を持つ値 $\beta$ （以下、相関値 $\beta$ という）、復号鍵と相関を持つ値 $\gamma$ （以下、相関値 $\gamma$ という）のうちの1つを選択する選択回路54と、選択回路54によって選択された相関値を復号鍵に変換する変換回路21と、復号鍵を用いて暗号化されたデータ16または暗号化されたプログラム17を復号化する復号回路22とを含んでいる。

【0055】復号鍵選択情報55は、復号装置12の外部から入力される。一方、相関値 $\alpha$ 、相関値 $\beta$ 、相関値 $\gamma$ は、いずれも、復号装置12の内部に格納されている。相関値 $\alpha$ 、相関値 $\beta$ 、相関値 $\gamma$ を復号装置12の内部に格納する方法としては、上述した復号鍵情報42を復号装置12の内部に格納する方法と同様の方法が採用され得る。例えば、相関値 $\alpha$ 、相関値 $\beta$ 、相関値 $\gamma$ をプロセッサチップ11に設けられているROM（図示せず）に格納する場合には、相関値 $\alpha$ はROMの格納位置56に格納され、相関値 $\beta$ はROMの格納位置57に格納され、相関値 $\gamma$ はROMの格納位置58に格納され得る。

【0056】図6に示す例では、図5に示される復号鍵 $\alpha$ 、復号鍵 $\beta$ 、復号鍵 $\gamma$ の代わりに、相関値 $\alpha$ 、相関値 $\beta$ 、相関値 $\gamma$ が復号装置12の内部に格納されているため、第三者が復号鍵選択情報55を得た場合でも復号鍵を知ることは一層困難である。

【0057】次に、図6を参照して、復号鍵選択情報55が入力された場合の復号装置12の動作を説明する。

【0058】選択回路54は、復号鍵選択情報55に応じて、相関値 $\alpha$ 、相関値 $\beta$ 、相関値 $\gamma$ のうちの1つを選択する。例えば、選択回路54は、復号鍵選択情報55が値0を有する場合に相関値 $\alpha$ を選択し、復号鍵選択情報55が値1を有する場合に相関値 $\beta$ を選択し、復号鍵選択情報55が値2を有する場合に相関値 $\gamma$ を選択する。復号鍵選択情報55の値と選択されるべき相関値との対応関係は任意に設定され得る。変換回路21は、選択回路54によって選択された相関値を復号鍵に変換する。復号回路22は、復号鍵を用いて暗号化されたデータ16または暗号化されたプログラム17を復号化する。その結果、復号化されたデータ16aまたは復号化されたプログラム17aが復号回路22から出力される。

【0059】なお、復号装置12の内部に格納される相関値の数は3に限定されない。復号装置12の内部に格納される相関値の数は任意の正の整数であり得る。

【0060】なお、相関値の代わりに、相関値とダミーデータとを含む復号鍵情報を復号装置12の内部に格納するようにしてもよい。この場合には、復号鍵情報から相関値を抽出する抽出回路を変換回路21の前段に設け

ればよい。また、復号鍵選択情報55がダミーデータを含んでいてもよい。この場合には、復号鍵選択情報55から相関値に対応する値を抽出する抽出回路を選択回路54の前段に設ければよい。

【0061】なお、図4～図6に示される実施の形態を任意に組み合わせた実施の形態も、本発明の範囲に含まれる。

【0062】（実施の形態3）図7は、復号装置12の他の構成を示す。図7に示される復号装置12は、プログラム保存用メモリ61にアドレスを提供するアドレスシャッフル回路62と、暗号化されたプログラム17のうちアドレスによって指定される命令を復号化する復号回路22とを含んでいる。

【0063】プログラム保存用メモリ61は、プロセッサチップ（図1）の内部に設けられていてもよく外部に設けられていてもよい。プログラム保存用メモリ61は、復号装置12の内部に設けられていてもよく外部に設けられていてもよい。暗号化されたプログラム17は、復号装置12に関連して設けられたプログラム保存用メモリ61に格納されている。

【0064】次に、図7を参照して、復号装置12の動作を説明する。

【0065】アドレスシャッフルを行わない場合には、アドレスシャッフル回路62を介することなくプロセッサコア15（または図示しないプログラムローダ）からプログラム保存用メモリ61にアドレスがシーケンシャルに出力される。そのアドレスに従って暗号化されたプログラム17の命令がシーケンシャルにプログラム保存用メモリ61から読み出され、復号回路22に供給される。復号回路22は、復号鍵情報18に応じて、暗号化されたプログラム17のうちアドレスによって指定された命令を復号化する。この場合、プログラム保存用メモリ61には暗号化されたプログラム17の命令をシーケンシャルに予め書き込んでおく必要がある。

【0066】アドレスシャッフルを行う場合には、プロセッサコア15（または図示しないプログラムローダ）からシーケンシャルに出力されたアドレスがアドレスシャッフル回路62に入力される。アドレスシャッフル回路62は、入力されたアドレスを一定の規則に従って変換し、変換されたアドレスをプログラム保存用メモリ61に出力する。その変換されたアドレスに従って暗号化されたプログラム17の命令がプログラム保存用メモリ61から読み出され、復号回路22に供給される。復号回路22は、復号鍵情報18に応じて、暗号化されたプログラム17のうちアドレスによって指定された命令を復号化する。この場合、プログラム保存用メモリ61には暗号化されたプログラム17の命令をアドレスシャッフル回路62におけるアドレス変換の特性を考慮して予め書き込んでおく必要がある。

【0067】アドレスシャッフル回路62におけるアド

レス変換の方法としては、様々な方法が採用され得る。例えば、その方法は、偶数アドレスを奇数アドレスに変換し、奇数アドレスを偶数アドレスに変換するといった規則的にアドレスをシャッフルする方法であってもよく、まったくランダムにアドレスをシャッフルする方法であってもよい。

【0068】なお、復号鍵情報18を復号回路22に直接的に入力する代わりに、図2(a)に示す構成と同様の構成によって復号鍵情報18から復号鍵18aを得て、復号鍵18aを復号回路22に入力するようにしてもよい。あるいは、復号鍵情報18を復号鍵情報41と復号鍵情報42とに分割して、図4に示す構成と同様の構成によって復号鍵情報41と復号鍵情報42とから復号鍵18aを得て、復号鍵18aを復号回路22に入力するようにしてもよい。あるいは、復号鍵情報18を使用することなく、図5に示す構成と同様の構成によって選択される復号鍵を復号回路22に入力するようにしてもよい。あるいは、復号鍵情報18を使用することなく、図6に示す構成と同様の構成によって得られる復号鍵を復号回路22に入力するようにしてもよい。

【0069】なお、暗号化されたデータを格納するデータ保存用メモリを設け、アドレスシャッフル回路62がそのデータ保存用メモリにアドレスを提供するようにしてもよい。

【0070】(実施の形態4)以下、本発明の復号装置を含むプロセッサチップを実際のアプリケーションに適用する形態を説明する。

【0071】図8は、電子バンキングシステム400の構成を示す。電子バンキングシステム400は、送信側のプロセッサチップ71と受信側のプロセッサチップ11とを含んでいる。プロセッサチップ71とプロセッサチップ11とは、通信回線410を介して互いに接続されている。

【0072】プロセッサチップ71は、暗号装置72とインタフェース73とプロセッサコア75とを含む。インタフェース73は、バス74を介して暗号装置72に接続されている。暗号装置72は、暗号鍵を用いて電子バンキングデータを暗号化する暗号回路(図示せず)を含んでいる。

【0073】プロセッサチップ11は、復号装置12とインタフェース13とプロセッサコア15とを含む。インタフェース13は、バス14を介して復号装置12に接続されている。復号装置12は、復号鍵を用いて暗号化された電子バンキングデータを復号化する復号回路

(図示せず)を含んでいる。ここで、復号回路において使用される復号鍵と暗号回路において使用される暗号鍵とは同一である。復号装置12は、実施の形態1および実施の形態2において説明した任意の構成を有し得る。

【0074】次に、コンピュータネットワーク上で電子バンキングデータを通信する場合におけるプロセッサチ

ップ71およびプロセッサチップ11の動作を説明する。

【0075】プロセッサチップ11は、通信回線410を介してプロセッサチップ71に復号鍵情報77を送信する。

【0076】プロセッサチップ71は、通信回線410を介して復号鍵情報77を受信する。復号鍵情報77は、インタフェース73を介して暗号装置72に入力される。また、電子バンキングデータ78は、プロセッサチップ71のプロセッサコア75に入力される。プロセッサコア75は、必要に応じて、電子バンキングデータ78を処理する。プロセッサコア75から出力される電子バンキングデータ78は、暗号装置72に供給される。暗号装置72は、復号鍵情報77に応じて、電子バンキングデータ78を暗号化する。その結果、暗号化された電子バンキングデータ76が得られる。プロセッサチップ71は、暗号化された電子バンキングデータ76を通信回線410を介してプロセッサチップ11に送信する。

【0077】プロセッサチップ11は、通信回線410を介して暗号化された電子バンキングデータ76を受信する。暗号化された電子バンキングデータ76は、復号装置12に入力される。復号装置12は、復号鍵情報77に応じて、暗号化された電子バンキングデータ76を復号化する。その結果、電子バンキングデータ78が得られる。プロセッサコア15は、必要に応じて、電子バンキングデータ78を処理する。プロセッサコア15から出力される電子バンキングデータ78は、プロセッサチップ11の外部に出力され得る。

【0078】このように、通信回線410上で通信される電子バンキングデータを暗号化することにより、電子バンキングデータ78の秘匿性を高くすることができる。実施の形態1で述べたように復号鍵情報77にダミーデータを挿入することにより、電子バンキングデータ78の秘匿性をさらに高くすることができる。実施の形態2で述べたように復号装置12の外部から入力される復号鍵情報77と復号装置12の内部に格納されている復号鍵情報とに基づいて、暗号化された電子バンキングデータ76を復号化するために使用される復号鍵を生成することにより、電子バンキングデータ78の秘匿性をさらに高くすることができる。

【0079】なお、プロセッサチップ71とプロセッサチップ11との間で通信を行う際に使用される媒体は、通信回線に限定されない。そのような通信媒体は、ICカードなどの磁気メディアや、光ディスクであってもよい。通信媒体として、磁気メディアや光ディスクを使用する場合には、それらに復号鍵情報を予め記憶させておく必要がある。

【0080】さらに、暗号化されたデータの代わりに、暗号化されたプログラムをプロセッサチップ71とプロ

セッサチップ11との間で通信することも考えられる。例えば、そのプログラムの処理内容を受信側に知られたくない場合には、暗号化されたプログラムをプロセッサチップ71とプロセッサチップ11との間で通信し、かつ、復号化されたプログラムをプロセッサチップ11の外部に出力しないように、プロセッサチップ71とプロセッサチップ11とを構成することが好ましい。そのようなプログラムの例としては、例えば、映像処理のプログラムが挙げられる。

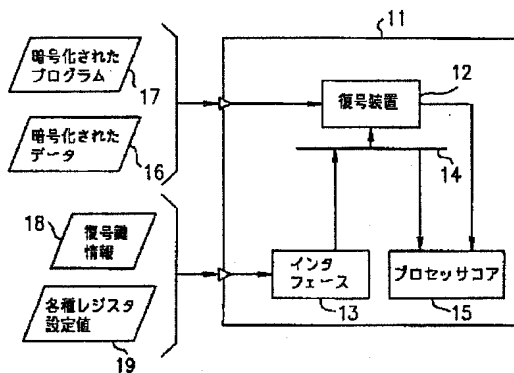
#### 【0081】

【発明の効果】本発明の復号装置によれば、復号鍵を用いて暗号化されている情報が復号化される。その復号鍵は第1復号鍵情報と第2復号鍵情報とに基づいて生成される。第1復号鍵情報は復号装置の外部から入力され、第2復号鍵情報は復号装置の内部に格納されている。このように、復号鍵を生成するために使用される情報の一部（すなわち、第2復号鍵情報）が復号装置の内部に格納されているため、第三者が第1復号鍵情報を得た場合でも復号鍵を知ることが困難である。これにより、復号装置の外部から入力される第1復号鍵情報の機密レベル

を下げることができる。その結果、第1復号鍵情報を復号装置に転送するために必要とされる回路の規模を削減することができる。

【0082】本発明の他の復号装置によれば、復号鍵を用いて暗号化されている情報が復号化される。その復号鍵は復号鍵情報を変換することによって得られる。その復号鍵情報は、復号鍵に関連する情報と復号鍵に関連しないダミーデータとを含んでいる。復号鍵情報には復号鍵に関連しないダミーデータが含まれているため、第三者が復号鍵情報を得た場合でも復号鍵情報に含まれる復\*

【図1】



\* 号鍵に関連する情報を特定することは困難である。これにより、復号鍵情報の機密レベルを下げることができる。その結果、復号鍵情報を復号装置に転送するために必要とされる回路の規模を削減することができる。

#### 【図面の簡単な説明】

【図1】本発明の復号装置12を含むプロセッサチップ11の構成を示す図である。

【図2】(a)は復号装置12の構成を示す図、(b)および(c)は復号鍵情報18の構成例を示す図である。

【図3】抽出回路26に入力される復号鍵情報18のタイミングとタイミング調整回路27から出力されるインーブル信号のタイミングとの関係を示す図である。

【図4】復号装置12の他の構成を示す図である。

【図5】復号装置12の他の構成を示す図である。

【図6】復号装置12の他の構成を示す図である。

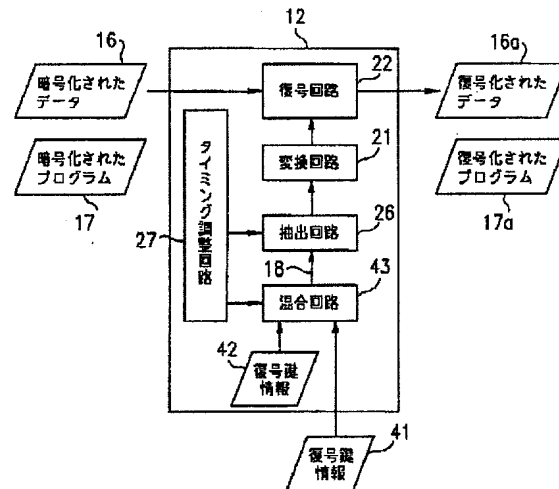
【図7】復号装置12の他の構成を示す図である。

【図8】電子バンキングシステム400の構成を示す図である。

#### 【符号の説明】

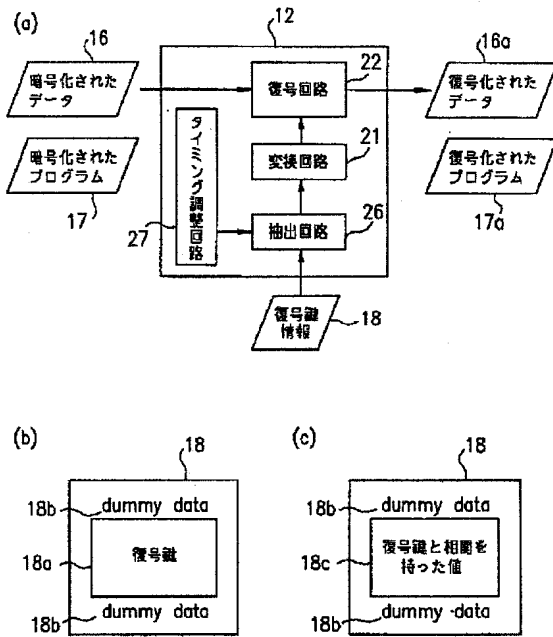
- 11 プロセッサチップ
- 12 復号装置
- 13 インタフェース
- 14 バス
- 15 プロセッサコア
- 16 暗号化されたデータ
- 17 暗号化されたプログラム
- 18 復号鍵情報
- 19 各種レジスタ設定値

【図4】

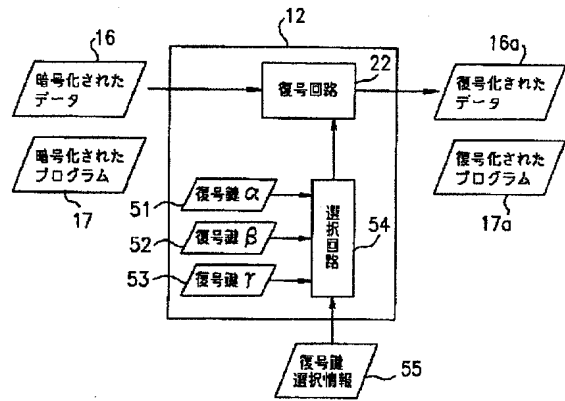




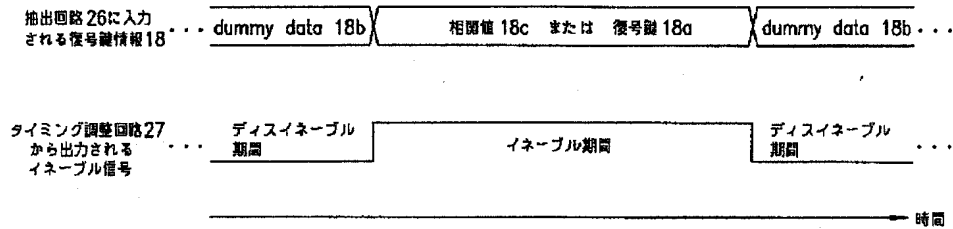
【図2】



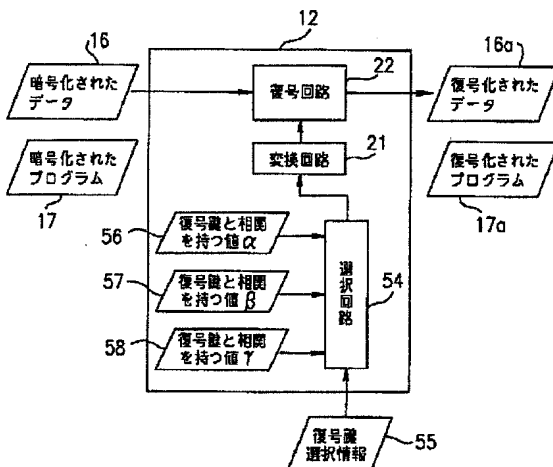
【図5】



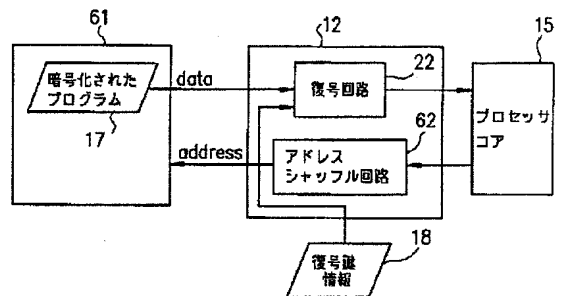
【図3】



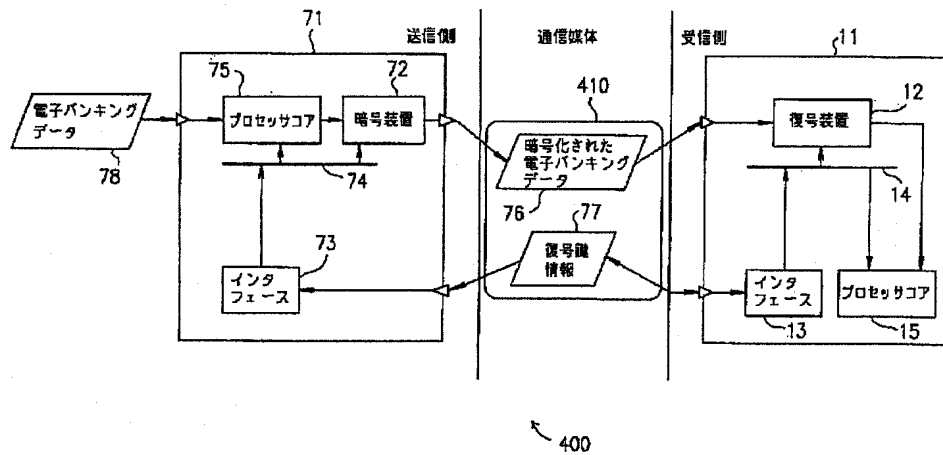
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 ▲徳▼永 尚哉  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 寒川 賢太  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72)発明者 宮口 裕  
東京都港区北青山3丁目6番12号 青山富  
士ビル 日本テキサス・インスツルメンツ  
株式会社内